METHOD AND SYSTEM FOR STATISTICALLY BASED PROTECTION OF HOST DEVICE FROM FLOOD ATTACKS

FIELD OF THE INVENTION

[01] The present invention generally relates to enhancing the protection of a host computer from network disruptions, more particularly to a method and system that protects a server from flooding attacks on the Internet.

BACKGROUND OF THE INVENTION

[02] The Internet has become an integral part of the modern society. Numerous consumers use the Internet to, among other things, purchase products on-line, locate special events, read news stories, pay bills or perform on-line banking. Numerous business establishments are connected to the Internet to provide products and services to the consumer or perform business-to-business electronic commerce. E-commerce and Internet applications operate and transmit data over a world-wide interconnected communications network. The applications on the Internet and World Wide Web transmit data over this interconnected communications network via a Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP protocol was created in the early 1970's and has evolved into a transportation protocol to conduct numerous electronic transactions.

[03] Unfortunately, the TCP/IP protocol causes the devices, such as servers, connected to the Internet to be vulnerable to computer hacker attacks. These computer hacker attacks have been increasing in recent years over the Internet. A denial-of-service (DoS) attack is one type of attack that disables servers connected to the Internet, denying users access to the victimized server because of data connection overloading. These attacks are not only frustrating for users trying to access the servers under attack, but are also expensive for the businesses operating the servers. The costs of these attacks can be measured in lost revenues and numerous manpower hours to fight the attacks.

[04] Servers in a network may be vulnerable to a form of a denial of service attack commonly called a "SYN attack" that occurs during a three-way handshake operation used for starting a data connection between two devices (the client and the host) over the Internet or in an IP network. In an IP network operating in a normal mode, the communication setup procedure between a client and a host computer/server (i.e., at the TCP layer) calls for a three-way handshake as three data messages -- a client SYNchronize, a server SYNchronize and ACKnowledge, and a client ACKnowledge -- are exchanged before a data transfer session begins. For example, in a first step, the client sends a TCP SYN segment carrying a sequence number to the server. In a second step, after the server receives the SYN segment, the server then sends a TCP SYN message carrying the sequence number and an ACK to the client. In a third step, when the client TCP receives the server's SYN/ACK message, the client transmits a TCP ACK to the server. After the three-way handshake is completed, the client and server switch to a data transfer/connection mode to send and receive application(s) data.

[05] In the above three-way handshake scheme, if the client TCP does not send the last ACK message to the server, the server TCP continues to wait for the arrival of the ACK message until a timeout period ends. A timer expires after the timeout period and, upon the expiration of time, moves the server back to a closed connection state. The denial-of-service problem arises when a client application "floods" the server with a large number of connection establishment requests in a relatively short time period without actually sending back the last ACK message, which results in a failure to complete the three-way handshake. As a result, the server is continually waiting for the ACK message from each connection establishment request. In this case, the server becomes swamped with the numerous connection establishment requests and continues to wait with open connections and can be easily paralyzed.

[06] There does not appear to be an effective way to predict when these SYN attacks are occurring at a particular host computer. Unfortunately, a SYN attack is

generally discovered after substantial damage to the victimized host computer has already occurred. Thus, it is desirable to predict when a SYN attack is occurring in real-time, prior to the host computer being disabled. It is also desirable to reduce the manpower and labor hours associated with correcting the disabled server. Accordingly, there appears to be lacking an existing way of predicting when a SYN attack is occurring at a particular host computer so that the host computer is enabled to self-adjust to take protective actions based on the predicted SYN attack.

[07] Traffic engineering employs statistical methods to estimate traffic flow between points on a telephone network. In using traffic engineering, two patents describe methods of detecting mass addressing events, such as dialing that overloads or shuts down network switching equipment. The U.S. Patent No. 5,864,611 to Ching et al. discloses a system and method for estimating traffic rates in a telephone network. U.S. Patent 5,923,742 to Kodialam et al. describes a method to detect mass addressing events and is aimed at alerting telephone network operations centers. While these patents detect or estimate traffic rates on phone networks, these patents do not describe methods of protecting IP networks or methods of protecting a host computer from a flooding attack.

BRIEF SUMMARY OF THE INVENTION

[08] Briefly, the present invention overcomes the problems in the art by providing a system and method of predicting and protecting a host computer or device from a flooding attack. In accordance with a first aspect of the invention, there is provided a method for receiving a first request from a client for starting a first data connection. The first request may be an initializing SYN request for a three-way handshake operation as in the TCP/IP protocol. The method further comprises the step of receiving a second request from the client for starting a second data connection. Likewise, the second request can be a SYN request. The arrival times at the host computer or device of the first and second requests are obtained and retained. Next, the method includes the step of determining if a calculated difference in the arrival times between the first request and the second

request is less than or equal to a predetermined time period. The predetermined time interval has a value based on a probability distribution function of the arrival times of previous connection establishment requests received at the host device from an originating network address. Therefore, if the calculated difference is less than or equal to the predetermined time interval, transmission of a synchronize message to the client is prevented. In this way, a potential flooding attack is predicted so that a multiplicity of the initializing SYN messages from the same client is prevented from disabling a host computer.

[09] In accordance with a second aspect of the invention, there is provided a method of protecting a host device from a flooding event in a telecommunications network. The method includes receiving an initialization request from a client for starting a data transmission session. Next, the method includes the step of determining whether the originating address of the client that sent the request has been previously received within a predetermined time period. The predetermined time period has a value based on a probability distribution function of the inter-arrival times of previous initializing requests of data transmission sessions received at the host device. If the originating address of the client has been previously received within the predetermined time period, then the most recent initializing request for data transmission session is denied to the client. In one case, this denial includes preventing transmission of a synchronization message to the client from the host device. In this manner, a flooding attack or event is prevented from disabling the host device.

[10] According to a third aspect of the invention, there is provided a system for protecting a host device from a flooding event. The system includes a processing device for processing and receiving a first request from a client for starting a first data session and a second request from the client for starting a second data session. A program that is embodied in computer-readable code cooperates with the processing device to execute steps of receiving a first request from a client for starting a first data connection and a second request from the client for starting a second data connection and evaluating the arrival times of

the first request and the second request against a predetermined time value based on a probability distribution function fitted to a plurality of inter-arrival times of previous data connection requests received at the host device from a given originating client so that the second data connection to the client is denied, provided that the arrival times of the first request and the second request are less than or equal to the predetermined time value. In this manner, a system can be provided in the host device or upstream of the host device for protection from a flooding event.

[11] According to a fourth aspect of the invention, there is provided a method of protecting a host device from a flooding event. In the method, the host device receives a first request from a client for starting a first data connection and a second request from the client for starting a second data connection. The arrival times of the first request and the second request are evaluated against a predetermined time value that is based on a probability distribution function fitted to a plurality of inter-arrival times of data connection requests received at the host device from a given originating client. Then responsive to the step of evaluating, a network control center is signaled if the arrival times of the first request and the second request are at least less than or equal to the predetermined time value. In this manner, a potential flooding attack is predicted so that initializing SYN messages from the same client received in a short time period are prevented from disabling a host computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[12] The foregoing summary of the invention, as well as the following detailed description of the preferred embodiments, is better understood when read in conjunction with the accompanying drawings, which are included by way of example and not by way of limitation with regard to the claimed invention:

[13] FIG. 1 is a schematic diagram of a telecommunication network environment in which an embodiment of the present invention may be implemented;

[14] FIG. 2 is a schematic diagram of an embodiment of a method of operating a host computing device according to the teaching of the present invention; and

[15] FIG. 3 is an example of traffic rate data in a host computing device in a normal mode of operation.

DETAILED DESCRIPTION OF THE INVENTION

[16] FIG. 1 illustrates a high-level system architecture environment for implementing a preferred embodiment of a system and method of the present invention. In general, client applications 1_1, 1_2 ... 1_7 transmit connection establishment requests in the form of data packets to a telecommunications network 3. Network 3 comprises hardware and software for transmission of data packets across the network. Network 3 includes a plurality of routing switches 5 for transmitting and routing data packets to a local area network ("LAN") or enterprise network 7. Local area network 7 provides network connectivity and routing of data packets to one or more host computers or destination servers 9_1, 9_2, 9_3, and 9_4. Networks 3 and 7 may have an Internet protocol component, such as TCP/IP.

[17] Host computers 9_1-9_4 may execute one or more application programs a, b, and c, such as web-applications for displaying web pages and/or conducting electronic commerce transactions. As can be appreciated by one of ordinary skill in the art, each host computer 9_1-9_4 may be a general-purpose computing device, including one or more central processing units (not shown), a system memory (not shown), and a system bus (not shown) that couples various system components, including the system memory, to the central processing unit. The system bus may be any one of several types of bus structures. The general purpose computing device may use any number of operating systems, such as MICROSOFT WINDOWS®, WINDOWS NT®, UNIX®, SOLARIS®, REDHAT® or LINUX® or other variations. The system memory typically includes read only memory ("ROM") and random access memory ("RAM"). The general-purpose computing device can be any host computer system configured to operate with devices using the TCP/IP protocol. It should be recognized that the host computer includes

networking software and a network interface for sending and receiving data packets to and from network 3 and 7.

[18] With reference to FIG. 1, host computers 9_1-9_4 also include a computer-readable storage device having one or more magnetic disk drives or optical disk drives, such as Compact Disk ROM, or DVD drives. According to an embodiment of the invention, the computer-readable storage device includes a computer-readable medium containing programmed steps for execution on the central processing unit of an embodiment of a method of protecting the host computers from a large number of connection requests in a relatively short time period from the same client application. The computer-readable medium provides nonvolatile storage of computer-readable code.

[19] FIG. 2 illustrates an embodiment of a method of providing an electronic barrier or an electronic dam (e-dam) to protect designated servers from a flooding attack originating from a client connected to IP networks, such as the Internet and client applications, such as the World Wide Web. In sum, to protect the servers or host computers 9_1-9_4, the data traffic received at the computers is captured and analyzed by various statistical methods. As shown in FIG. 1, client application 1_5 may be responsible for sending a large quantity of SYN requests to host computer 9_4. The probability distribution of times between the reception or arrival of data packets from an originating IP address (e.g., client application 1_5) to a destination IP address, (e.g., IP server 9_4) can be approximated with a number of configuration-dependent analytic approaches. In one approach, an appropriate Gamma-distribution can be fitted to the inter-arrival times so as to determine the probability of receiving data packets from a given originating client application for a specific value of a predetermined time period.

[20] More specifically, in a normal mode of operation, the likelihood or chance that a host computer receives consecutive SYN requests, such as a first SYN request and a second SYN request, within certain time intervals from the same originating client can be determined from traffic rate data at the host computer.

For ease of explanation, a normal mode of operation can be defined as traffic rate data at the host computer for uses not including flooding attack data.

[21] According to an embodiment of the invention, a probability distribution of previous inter-arrival times can be applied to predicting flooding attack traffic, in which many SYN requests from the same client occur within a small time interval that is out of the ordinary for a normal mode of the operation of the data traffic for the particular host computer. As explained below, this time interval is used as at least one basis for protecting host computers 9_1-9_4 from a flooding attack, in particular a denial of service attack in the form of a SYN attack. It should be recognized that the probability distribution is dependent on a number of parameters, such as the type of traffic being received by host computers 9_1-9_4 and type of the application programs being executed on the host computers.

[22] With continued reference to FIG. 2, at block 101, a connection establishment request in the form of a data packet or packets is received by host computer 9_4 from at least one client 1_5 (see FIG. 1) for starting a three-way handshake operation in the TCP/IP protocol stack. In one embodiment, the data packet is an initializing SYN request from the client application.

[23] At block 103, the Internet Protocol (IP) address of the client application is obtained from the data packet or by other known methods and the IP address with the arrival time is temporarily stored in the system memory or a computer-readable storage device of the host computer. In addition, the IP address of the client application (e.g., client 1_5) that transmitted the connection establishment request is compared to each element in a list containing IP addresses of connection establishment requests that have been previously received by host computer 9_4 within a predetermined time period *t*. This operation is performed to determine whether the client application IP address has been previously received within the predetermined time period *t*.

[24] Program flow proceeds to block 105 so that, based on the calculated time difference, a decision is made as to whether the time difference is less than or equal to the predetermined time period *t*.

[25] At block 107, based on the results of the operation in block 105, if the time difference is indeed less than or equal to the predetermined time period *t*, this indicates that a potential flooding attack is occurring. To protect the server (e.g., server 9_4) from this flooding attack, the server denies or terminates the three-way handshake operation of the most recent connection establishment request received from the same client application.

[26] With continued reference to block 107, in one embodiment, the denial of the connection establishment request is accomplished by preventing the server from transmitting or otherwise sending a SYN message to the client application. It should be recognized that the terms "SYN" and "ACK" refer to the TCP/IP protocol designation and that messages having equivalent functions in the three-way handshake operation are considered to be within the scope of the invention. Nevertheless, in a flooding attack, the approach identified here can protect against the following: a hacker wanting to flood a server (e.g., server 9_4) has held the last client ACK step from sequence that is used by the TCP/IP protocol during the connection establishment phase (e.g., 3-way handshake), thereby making the server wait for the timeout period to expire.

[27] According to an embodiment, a signal may be transmitted to a network control center ("NCC") 11 (see FIG. 1) before, during or after the data connection is denied to the client. Network control center 11 includes hardware and software that can control the various devices within networks 3 and 7, such as routers 5. The network control center may be connected to network 3 or local area network 7. The signal may be an e-mail sent to a receiving computer in the NCC 11. Alternatively, the signal may be an automated telephone call to the center, a message sent to a wireless pager or any other alert signaling messaging method. This arrangement can help network control center 11 to take corrective action against the identified client, such as barring data originating at the client IP

address from entering the network or reaching the server. This action may be accomplished by downloading from the NCC 11 appropriate commands to the server and appropriate commands to specific switching devices in the network. Alternatively, the NCC 11 is enabled to send appropriate commands to one or more hot standby host/servers to take over the function performed by the host device that was shutdown. This arrangement provides for uninterruptible service to the users accessing the host device which was subjected to the flooding attack.

[28] Turning again to program flow from block 105, as shown in block 109, if the time difference between the most recent receipt time of the SYN request from the same client or originating client and the prior receipt time of the prior SYN request from the client is greater than predetermined time period *t*, then a data connection is allowed to proceed. Specifically, a SYN message is transmitted to the client having the IP address that sent the most recent SYN request. In addition, the IP address of the client is stored or saved on the list of recent connection establishment requests. At reasonable regular intervals, the IP address(es) of the client(s) and receipt of the prior SYN request(s) are cleared from the list, because they may be considered aged and are subsequently dropped. The length of this interval is a parameter that may be established by a network administrator or other appropriate method. This clearance function is desirable to keep the list current to the most recent SYN requests from the same client or clients. Then at block 111, the server proceeds to process the next data packet.

[29] In a further embodiment of the present invention, the central processor of the respective host computers 9_1-9_4 executes a step of determining a probability distribution of the inter-arrival times of a plurality of the initialization requests and a plurality of previous received initialization requests from a client to a destination server within certain values of the predetermined time period. In addition, the probability distribution of the inter-arrival times of connection establishment requests from the same client application is analyzed at the destination server so as to determine a predetermined time period *t* for a given

value of a predetermined probability value p. As an example, the predetermined time period t may be equal to 1 millisecond for a predetermined probability value of 1%. In another example, a most recent SYN request from the same client IP address is rejected if the prior SYN request arrived within 1 millisecond.

[30] By way of illustrating one example of obtaining a predetermined time period, FIG. 3 shows a time line distribution of inter-arrival times between data flows versus the probability of inter-arrival times greater than t of at least two data packets between a given pair of IP addresses. The given pair of IP addresses may originate from a sending device having an originating IP address and a receiving device having a destination IP address. For ease of explanation, the sending device may be a client and the receiving device may be a server or a host computer. From reviewing the data, it can be seen that less than 1% of the consecutive flows between any pair of IP addresses have arrived within 1 millisecond and only 5% of the consecutive flows have arrived within 201 milliseconds. As shown in FIG. 3, for any value of probability, a time interval can be calculated so that the probability of two traffic data flows starting from any given IP address and received at another given IP address within a predetermined time interval is less than the given value of probability. It should be recognized that the shorter the time interval, the lower the probability of receiving two or more connection requests from the same client within this time interval, hence lessening the odds of flooding the computer with an attack.

[31] Thus, a system and method of predicting and protecting a host computer from a flooding attack has been described that can be applied in any e-commerce environment that is accessed by client applications. It should be recognized that, if desired, the present methods can be implemented within the host computer or within a device upstream of the host computer having sufficient computer processing power to analyze the data and execute program steps. It is also contemplated that an embodiment of the invention may be added or adapted to

the TCP/IP implementations, including network operating software to enhance the robustness and to reduce the vulnerability of the implementation.

[32] While the flooding attack can be predicted and stopped by the illustrated methods, it is acknowledged that a predetermined threshold *t* can account for rejecting possible non-flooding type of requests. By using the predetermined threshold *t*, the system accepts that some legitimate SYN requests that have a difference in arrival times less than predetermined time period *t* may be rejected. Nevertheless, in a protection system as disclosed, a very low number of possible rejections are acceptable to prevent a SYN flooding attack from disabling the destination server.

[33] While the present invention has been described with reference to preferred and exemplary embodiments, it will be understood by those of ordinary skill in the art that various changes may be made and equivalents may be substituted for elements thereof without departing from the scope of the invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the invention without departing from the scope. Therefore, it is intended that the invention not be limited to the particular embodiment disclosed, but that the invention include all embodiments falling within the scope of the appended claims.